# Embedded SFE: Offloading Server and Network using Hardware Tokens
(Full Version)[⋆]

Kimmo Järvinen[1], Vladimir Kolesnikov[2], Ahmad-Reza Sadeghi[3], and Thomas Schneider[3]

[1] Dep. of Information and Comp. Science, Aalto University, Finland
`kimmo.jarvinen@tkk.fi`[⋆⋆]
[2] Bell Laboratories, 600 Mountain Ave. Murray Hill, NJ 07974, USA
`kolesnikov@research.bell-labs.com`
[3] Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany
{`ahmad.sadeghi,thomas.schneider`}`@trust.rub.de`[⋆⋆⋆]

**Abstract.** We consider Secure Function Evaluation (SFE) in the client-server setting where the server issues a secure token to the client. The token is not trusted by the client and is *not* a trusted third party.
We show how to take advantage of the token to drastically reduce the communication complexity of SFE and computation load of the server.
Our main contribution is the detailed consideration of design decisions, optimizations, and trade-offs, associated with the setting and its strict hardware requirements for practical deployment. In particular, we model the token as a computationally weak device with small constant-size memory and limit communication between client and server.
We consider semi-honest, covert, and malicious adversaries. We show the feasibility of our protocols based on a FPGA implementation.

## 1 Introduction

Secure and efficient evaluation of arbitrary functions on private inputs has been subject of cryptographic research for decades. In particular, the following scenario appears in a variety of practical applications: a service provider (server $\mathcal{S}$) and user (client $\mathcal{C}$) wish to compute a function $f$ on their respective private data, without incurring the expense of a trusted third party. This can be solved interactively using Secure Function Evaluation (SFE) protocols, for example using the very efficient garbled circuit (GC) approach [Yao86,LP09]. However, GC protocols potentially require a large amount of data to be transferred between $\mathcal{S}$ and $\mathcal{C}$. This is because $f$ needs to be encrypted (garbled) as $\widetilde{f}$ and transferred from $\mathcal{S}$ to $\mathcal{C}$. In fact, the communication complexity of GC-based SFE protocols is dominated by the size of the GC, which can reach Megabytes or Gigabytes

⋆ This paper will appear at FC 2010 [JKSS10].
⋆⋆ Supported by EU FP7 project CACE.
⋆⋆⋆ Supported by EU FP6 project SPEED, EU FP7 project CACE and ECRYPT II.

even for relatively small and simple functions (e.g., the GC for AES has size 0.5 MBytes [PSSW09]). Further, if security against more powerful adversaries is required, the use of the standard cut-and-choose technique implies transfer of multiple GCs. (For covert adversaries, the transfer of only one GC is sufficient [GMS08].)

While transmission of this large amount of data is possible for exceptional occurrences, in most cases, the network will not be able to sustain the resulting traffic. This holds especially for larger-scale deployment of secure computations, e.g., by banks or service providers, with a large number of customers. Additional obstacles include energy consumption required to transmit/receive the data, and the resulting reduced battery life in mobile clients, such as smartphones.[4]

Further, computational load on $\mathcal{S}$ (computing $\widetilde{f}$) is also a significant problem, especially in the case of large-scale deployment of SFE.

**Our setting, goals and approach.** Motivated by the possibility of large-scale and decentralized SFE deployment we aim to remove the expensive communication requirement, and to shift some of $\mathcal{S}$'s computation to $\mathcal{C}$. To this end, we note that in SFE protocols, and, in particular, in GC, the role of the server can be split between two entities, with the introduction of a new entity – secure token $\mathcal{T}$, which is placed in client $\mathcal{C}$'s possession, but executes $\mathcal{S}$'s code thus offloading $\mathcal{S}$. Further, it is possible to eliminate most of the communication between $\mathcal{C}$ and $\mathcal{S}$ and replace this with local communication between $\mathcal{C}$ and $\mathcal{T}$. A number of technical issues arises in this setting, which we address in this work.

More specifically, we discuss and analyze hardware-supported SFE, where the service provider $\mathcal{S}$ issues a *secure* (see below) hardware token $\mathcal{T}$ to $\mathcal{C}$. $\mathcal{C}$ communicates locally with $\mathcal{T}$, and remotely with $\mathcal{S}$. There is no direct channel between $\mathcal{T}$ and $\mathcal{S}$, but of course $\mathcal{C}$ can pass (and potentially interfere with) messages between $\mathcal{T}$ and $\mathcal{S}$. $\mathcal{T}$ is created by $\mathcal{S}$, so $\mathcal{S}$ trusts $\mathcal{T}$; however, as $\mathcal{C}$ does not trust $\mathcal{S}$, she also does not trust the token $\mathcal{T}$ to behave honestly.[5]

*Attack model.* We consider all three standard types of adversaries: semi-honest (follows protocol but analyzes the transcript), malicious (arbitrary behavior, cheating is always caught), and covert (cheating is caught with a certain deterrence probability, e.g., 1/2).

*Hardware assumption.* We assume $\mathcal{T}$ is tamper-proof or tamper-resistant. We argue that this assumption is reasonable. Indeed, while every token can likely be broken into, given sufficient resources, we are motivated by the scenarios where the payoff of the break is far below the cost of the break. This holds for relatively low-value transactions such as cell phone or TV service, where the potential benefit of the attack (e.g., free TV for one user) is not worth the

[4] In some cases, the impact can be mitigated by creating and transferring GCs in the precomputation phase. However, this is not fully satisfactory. Firstly, even more data needs to be transferred since demand cannot be perfectly predicted. Further, this creates other problems, such as requiring large long-term storage on client devices.

[5] Note, if $\mathcal{C}$ in fact trusts $\mathcal{T}$ to behave honestly, then there exists a trivial solution, where $\mathcal{C}$ would let $\mathcal{T}$ compute the function on her inputs [IS05].

investment of thousands or tens of thousands of dollars to break into the card. For higher-value applications one could raise the cost of the attack by using a high-end token $\mathcal{T}$, e.g., a smart card certified at FIPS 140-2, level 3 or 4.

*Hardware restrictions.* As we assume the token to be produced in large quantities, we try to minimize its costs (e.g., chip surface) and make the assumptions on it as weak as possible. In particular our token requires only restricted computational capabilities (no public-key operations) and small constant secure RAM. We consider $\mathcal{T}$ with and without small constant secure non-volatile storage.

Further, we envision smart phones playing the role of the client (and a SIM card the role of the token). Therefore we aim to limit client's computational power and storage ability.

**Envisioned Applications.** As mentioned above, we aim to bring SFE closer to a large-scale deployment. The need to minimize communication forces us to rely on tokens, the issuance of which requires certain logistical capabilities. Therefore, we believe client-server applications are most likely to be the early adopters of SFE. Further, the natural trust model (semi-honest or covert server and malicious client) allow for efficient GC protocols. Finally, many client-server application scenarios naturally include financial and other transactions which involve sensitive, in particular privacy-sensitive, information.

Today, many service providers already distribute trusted tokens to their users. Examples include SIM cards in users' cell phones, and smart cards in users' TV set-top boxes. Bank- and credit cards often contain embedded secure chips. Special purpose (e.g., diagnostic) medical devices, which need to be monitored and controlled, are often issued to users at home. In these settings, it is natural to use the existing infrastructure to enhance the security and privacy guarantees of the offered products, and to offer new products previously impossible due to privacy violation concerns. We consider the following examples in more detail.

*Privacy protection in targeted advertisement and content delivery.* Cable TV (phone, Internet) providers gain a large part of their revenue from advertisements, so it is desired to increase their effectiveness by considering individual user preferences, purchase history, and other collected personal information. On the other hand, privacy guidelines and laws severely limit the kinds of information that can be collected and how it can be used. Further, even legal use of personal information by the service provider may be viewed as privacy violation, and cause negative perception of the company. At the same time, using SFE to select advertisements guarantees customers' privacy, and, moreover, ensures that the company cannot breach their privacy policies even by accident.

Of course, other content (songs, movies, TV shows) can be target-delivered as rewards or incentives, while preserving complete privacy of the user. Discount coupons and certificates, powerful spending incentives well-liked by users, bring much more value to both issuer and the user, if their delivery is based on sensitive personal and location information.

*Privacy preserving remote medical diagnostics.* Healthcare is moving faster than ever toward technologies that offer personalized online self-service, medical error reduction, consumer data mining and more (e.g., [Goo09]). Such technologies have the potential of revolutionizing the way medical data is stored, processed, delivered, and made available in an ubiquitous and seamless way to millions of users all over the world. Here service provider $\mathcal{S}$ usually owns the diagnostic software and/or hardware that operates on $\mathcal{C}$'s data and outputs classification/diagnostic results. A concrete example in this context is the classification of Electrocardiogram (ECG) data. A privacy-enhanced version for remote ECG diagnostics requires to transfer GCs of size $\approx 63$ MBytes [BFK$^+$09]. With our token-based protocol this can be reduced substantially to approximately 100 kBytes as no garbled circuits need to be transferred.

Other applications concern *financial transactions* such as monetary transfers, bidding, or betting, as well as *biometric authentication.*

## 1.1 Our Contributions and Outline

Our main contribution is architecture design, implementation, a number of optimizations, and detailed analysis of two-party SFE aided by a server-issued low-cost tamper-proof token. The communication complexity of our protocols is linear in the size of the input, and is independent of the size of the evaluated functionality. Further, most of the work of $\mathcal{S}$ can be offloaded to $\mathcal{T}$.

We use GC techniques of [KS08] and offer no-cost XOR gates. We rely on cheap hardware – the token $\mathcal{T}$ only executes symmetric-key operations (e.g., SHA and AES). $\mathcal{T}$ has small constant-size RAM (much smaller than the size of the circuit), but we do not resort to implementing expensive secure external RAM. In appendix §A we also show how to optimize for low-power, low-memory $\mathcal{C}$.

We provide two solutions; in one, $\mathcal{T}$ keeps state in secure non-volatile storage (a monotonic counter), while in the other, $\mathcal{T}$ maintains no long-term state.

We consider semi-honest, covert [GMS08], and malicious [LP07] adversaries; our corresponding communication improvements are shown in Table 1.

**Outline.** We start with outlining our model and architecture in §3. We describe the protocols for both stateful and stateless $\mathcal{T}$, and state the security claim in §4. In §5, we discuss technical details of our FPGA prototype implementation, present timings and measurements, and show practicality of our solution.

**Table 1.** Communication between server $\mathcal{S}$ and client $\mathcal{C}$ for secure evaluation of function $f$ with $n$ inputs, statistical security parameter $s$, and deterrence probability $1-1/r$.

| Security | Previous Work | | This Work |
|---|---|---|---|
| semi-honest | [Yao86] | $\mathcal{O}(\|f\| + n)$ | $\mathcal{O}(n)$ |
| covert | [GMS08] | $\mathcal{O}(\|f\| + sn + r)$ | $\mathcal{O}(sn + r)$ |
| malicious | [LP07] | $\mathcal{O}(s\|f\| + s^2 n)$ | $\mathcal{O}(s^2 n)$ |

## 1.2 Related Work

Related work on using tokens for secure computations falls in the following three categories, summarized in Table 2.

**Table 2.** Secure Protocols using Hardware Tokens. Columns denote the number of tokens, who trusts the token(s), if token(s) are stateful or stateless, and perform public-key operations. Properties more desired for practical applications in bold font.

| Type | Reference | Functionality | # Tokens | Trusted by | Stateful | PK ops |
|---|---|---|---|---|---|---|
| A) | [HMU05] | UC commitment | 2 | both | yes | yes |
| | [Kat07,DNW09] | UC commitment | 2 | **issuer** | yes | yes |
| | [CGS08] | UC commitment | 2 | **issuer** | **no** | yes |
| | [MS08] | UC commitment | **1** | **issuer** | yes | **no** |
| B) | [HL08] | Set Intersection, ODBS | **1** | both | yes | **no** |
| | [GT08] | Non-Interact. OT | **1** | both | yes | yes |
| | [TV09] | Verif. Enc., Fair Exch. | **1** | both | yes | yes |
| C) | [FFP$^+$06] | **SFE** | 2 | both | yes | yes |
| | [IS05] | **SFE** | **1** | both | yes | yes |
| | This Work | **SFE** | **1** | **issuer** | yes / **no** | **no** |

*A) Setup assumptions for the universal composability (UC) framework.* As shown in [CLOS02], UC SFE protocols can be constructed from UC commitments. In turn, UC commitments can be constructed from signature cards trusted by both parties [HMU05], or from tamper-proof tokens created and trusted only by the issuing party [Kat07,MS08,CGS08,DNW09]. Here, [CGS08] consider stateless tokens, and [MS08] require only one party to issue a token. This line of research mainly addresses the feasibility of UC computation based on tamper-proof hardware and relies on expensive primitives such as generic zero-knowledge proofs. Our protocols are far more practical.

*B) Efficiency Improvements for Specific Functionalities.* Efficient protocols with a tamper-proof token trusted by both players have been proposed for specific functionalities such as set intersection and oblivious database search (ODBS) [HL08], non-interactive oblivious transfer (OT) [GT08], and verifiable encryption and fair exchange [TV09]. In contrast, we solve the general SFE problem.

*C) Efficiency Improvements for Arbitrary Functionalities.* Clearly, SFE is efficient if aided by a trusted third party (TTP), who simply computes the function. SFE aided by hardware TTP was considered, e.g., in [FFP$^+$06,IS05]. In contrast, we do not use TTP; our token is only trusted by its issuer.

## 2 Preliminaries

**Notation.** We denote symmetric security parameter by $t$ (e.g., $t = 128$), and pseudo-random function (PRF) keyed with $k$ and evaluated on $x$ by $\mathsf{PRF}_k(x)$. PRF can be instantiated with a block cipher, e.g., AES, or a cryptographic hash function $\mathsf{H}$, e.g., SHA-256, which we model as a Random Oracle (RO). AES is preferable if PRF is run repeatedly with same $k$ as AES's key schedule amortizes. Message authentication code (MAC) keyed with $k$ and evaluated on message $m$ is denoted by $\mathsf{MAC}_k(m)$. We use a MAC that does not need to store the entire message, but can operate "online" on small blocks, e.g., AES-CMAC [SPLI06] or HMAC [KBC97].

### 2.1 Garbled Circuits (GC)

Yao's Garbled Circuit approach [Yao86], excellently presented in [LP09], is the most efficient method for secure evaluation of a boolean circuit $C$. We summarize its ideas in the following. The circuit *constructor* (server $\mathcal{S}$) creates a *garbled circuit* $\widetilde{C}$: for each wire $w_i$ of the circuit, he randomly chooses two garblings $\widetilde{w}_i^0, \widetilde{w}_i^1$, where $\widetilde{w}_i^j$ is the *garbled value* of $w_i$'s value $j$. (Note: $\widetilde{w}_i^j$ does not reveal $j$.) Further, for each gate $G_i$, $\mathcal{S}$ creates a *garbled table* $\widetilde{T}_i$ with the following property: given a set of garbled values of $G_i$'s inputs, $\widetilde{T}_i$ allows to recover the garbled value of the corresponding $G_i$'s output, but nothing else. $\mathcal{S}$ sends these garbled tables, called *garbled circuit* $\widetilde{C}$ to the *evaluator* (client $\mathcal{C}$). Additionally, $\mathcal{C}$ obliviously obtains the *garbled inputs* $\widetilde{w}_i$ corresponding to inputs of both parties: the garbled inputs $\widetilde{y}$ corresponding to the inputs $y$ of $\mathcal{S}$ are sent directly and $\widetilde{x}$ are obtained with a parallel 1-out-of-2 oblivious transfer (OT) protocol [NP01,AIR01]. Now, $\mathcal{C}$ can evaluate the garbled circuit $\widetilde{C}$ on the garbled inputs to obtain the *garbled outputs* by evaluating $\widetilde{C}$ gate by gate, using the garbled tables $\widetilde{T}_i$. Finally, $\mathcal{C}$ determines the plain values corresponding to the obtained garbled output values using an output translation table received by $\mathcal{S}$. Correctness of GC follows from the way garbled tables $\widetilde{T}_i$ are constructed.

**Improved Garbled Circuit with free XOR [KS08].** An efficient method for creating garbled circuits which allows "free" evaluation of XOR gates was presented in [KS08]. More specifically, a garbled XOR gate has no garbled table (*no communication*) and its evaluation consists of XORing the its garbled input values (*negligible computation*) – details below. The other gates, called *non-XOR gates*, are evaluated as in Yao's GC construction [Yao86] with a *point-and-permute technique* (as used in [MNPS04]): The garbled values $\widetilde{w}_i = \langle k_i, \pi_i \rangle \in \{0,1\}^{t'}$ consist of a symmetric key $k_i \in \{0,1\}^t$ and a random permutation bit $\pi_i \in \{0,1\}$ (recall, $t$ is the symmetric security parameter). The entries of the garbled table are permuted such that the permutation bits $\pi_i$ of a gate's garbled input wires can be used as index into the garbled table to directly point to the entry to be decrypted. After decrypting this entry using the garbled input wires' $t$-bit keys $k_i$, evaluator obtains the garbled output value of the gate. The encryption is done with the symmetric encryption function $\mathsf{Enc}^s_{k_1,\ldots,k_d}(m)$, where $d$ is the number of inputs of the gate and $s$ is a unique identifier used once. $\mathsf{Enc}$ can be instantiated with $m \oplus \mathsf{H}(k_1||\ldots||k_d||s)$, where $\mathsf{H}$ is a RO. This requires $2^d$ invocations of $\mathsf{H}$ for creating and 1 invocation for evaluating a garbled non-XOR gate. To avoid random oracles, $\mathsf{Enc}$ can be instantiated with $m \oplus H(k_1||s) \oplus .. \oplus H(k_d||s)$ instead, where $H$ is a correlation robust hash function (cf. [PSSW09] for details). This needs $d \cdot 2^d$ invocations of $H$ for creating and $d$ invocations for evaluating a non-XOR gate. In practice, $H$ can be chosen from the SHA-2 family. The main observation of [KS08] is, that the constructor $\mathcal{S}$ chooses a global key difference $\Delta \in_R \{0,1\}^t$ which remains unknown to evaluator $\mathcal{C}$ and relates the garbled values as $k_i^0 = k_i^1 \oplus \Delta$. Clearly, the usage of such garbled values allows for *free evaluation of XOR gates* with input wires $w_1, w_2$ and output wire $w_3$ by computing $\widetilde{w}_3 = \widetilde{w}_1 \oplus \widetilde{w}_2$ (no communication and negligible computation).

## 3 Architecture, System and Trust Model

We present in detail our setting, players, and hardware and trust assumptions.

As shown in Fig. 1, there are three parties – client $\mathcal{C}$, server $\mathcal{S}$ and tamper-resistant token $\mathcal{T}$, issued and trusted by $\mathcal{S}$. Our goal is to let $\mathcal{C}$ and $\mathcal{S}$ securely evaluate a public function $f$ on their respective private inputs $x$ and $y$.

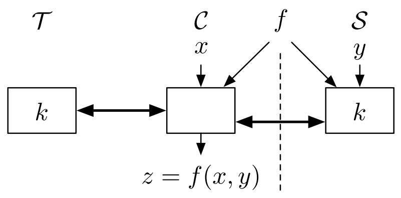


**Fig. 1.** Model Overview

**Communication.** $\mathcal{C} \leftrightarrow \mathcal{S}$: We view this as an expensive channel. Communication $\mathcal{C} \leftrightarrow \mathcal{S}$ flows over the Internet, and may include a wireless or cellular link. This implies small link bandwidth and power consumption concerns of mobile devices. We wish to minimize the utilization of this channel.

$\mathcal{T} \leftrightarrow \mathcal{C}$: As $\mathcal{T}$ is held locally by $\mathcal{C}$, this is a cheap channel (both in terms of bandwidth and power consumption), suitable for transmission of data linear in the size of $f$, or even greater.

$\mathcal{T} \leftrightarrow \mathcal{S}$: There is no direct channel between $\mathcal{T}$ and $\mathcal{S}$, but, of course, $\mathcal{C}$ can pass (and potentially interfere with) messages between $\mathcal{T}$ and $\mathcal{S}$.

**Trust.** $\mathcal{C} \leftrightarrow \mathcal{S}$: As in the standard SFE scenario, $\mathcal{C}$ and $\mathcal{S}$ don't trust each other. We address semi-honest, covert, and malicious $\mathcal{C}$ and $\mathcal{S}$.

$\mathcal{S} \leftrightarrow \mathcal{T}$: $\mathcal{T}$ is fully trusted by $\mathcal{S}$, since $\mathcal{T}$ is tamper-resistant. $\mathcal{S}$ and $\mathcal{T}$ share a secret key $k$, used to establish a secure channel and to derive joint randomness.

$\mathcal{T} \leftrightarrow \mathcal{C}$: $\mathcal{C}$ does not trust $\mathcal{T}$, as $\mathcal{T}$ is the agent of $\mathcal{S}$, and may communicate with $\mathcal{S}$ through covert channels.

**Storage, computation and execution.** $\mathcal{C}$ and $\mathcal{S}$ are computationally strong devices which can perform both symmetric- and asymmetric-key operations.[6] Both have sufficient memory, linear in the size of $f$. We also address the setting where $\mathcal{C}$ is a weak mobile device with restricted memory in appendix §A.1 $\mathcal{C}$ has control over $\mathcal{T}$, and can reset it, e.g., by interrupting its power supply. As justified in §1, $\mathcal{T}$ is a cheap special purpose hardware with minimum chip surface: $\mathcal{T}$ has circuitry only for evaluating symmetric-key primitives in hardware (no public-key or true random number generator) and has a small secure RAM. It may (§4.3) or may not (§4.4) have small non-volatile secure storage[7], unaffected by the resets by $\mathcal{C}$.

## 4 Token-Assisted Garbled Circuit Protocols

In our presentation, we assume reader's familiarity with the GC technique, including free XORs of [KS08] (cf. §2.1), and concentrate on the aspects specific to the token setting. We start with a high-level description of our protocol. Then, in §4.2 - §4.4, we present the technical details of our construction – efficient circuit representation, and GC generation by stateful and stateless tokens.

### 4.1 Protocols Overview, Security Intuition and Claim

Our constructions are a natural (but technically involved) modification of standard GC protocols, so as to split the actions of the server into two parts – now executed by $\mathcal{S}$ and $\mathcal{T}$ – while maintaining provable security. We offload most of the work (notably, GC generation and output) to $\mathcal{T}$, thus achieving important communication savings, and partially offloading $\mathcal{S}$'s computation to $\mathcal{T}$.

We start our discussion with the solution in the semi-honest model. However, our modification of the basic GC is secure against malicious actions, and our protocols are easily and efficiently extendible to covert and malicious settings.

At the high level, our protocols work as shown in Fig. 2: $\mathcal{C}$ obtains the garbled inputs $\widetilde{x}, \widetilde{y}$ from $\mathcal{S}$, and the garbled circuit $\widetilde{f}$ corresponding to the function $f$ from $\mathcal{T}$. Then, $\mathcal{C}$ evaluates $\widetilde{f}$ on $\widetilde{x}, \widetilde{y}$ and obtains the result $z = f(x, y)$.

It is easy to see that the introduction of $\mathcal{T}$ and offloading to it some of the computation does not strengthen $\mathcal{S}$, and thus does not bring security concerns for $\mathcal{C}$ (as compared to standard two-party GC). On the other hand, separating the states of $\mathcal{S}$ and $\mathcal{T}$, placing $\mathcal{C}$ in control of their communication, and $\mathcal{C}$'s ability to reset $\mathcal{T}$ introduces attack opportunities for $\mathcal{C}$. We show how to address these issues with the proper synchronization and checks performed by $\mathcal{S}$ and $\mathcal{T}$.

Our main tool is the use of a unique session id $\mathsf{sid}$ for each GC evaluation. From $\mathsf{sid}$ and the shared secret key $k$, $\mathcal{S}$ and $\mathcal{T}$ securely derive a session key $K$, which is then used to derive the randomness used in GC generation. Jumping ahead (details in §4.3), we note that $\mathsf{sid}$ uniqueness is easily achieved if $\mathcal{T}$ is

[6] If needed, $\mathcal{C}$'s capabilities may be enhanced by using a trusted hardware accelerator.
[7] $\mathcal{T}$'s key $k$ is a fixed part of its circuit, and is kept even without non-volatile storage.

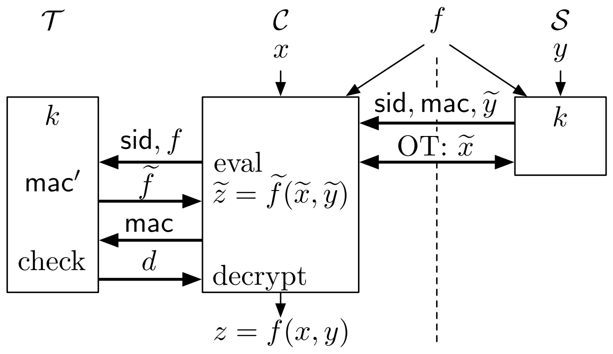


**Fig. 2.** Protocols Overview.

stateful simply by setting $\mathsf{sid}$ equal to the value of the strictly monotonic session counter $\mathsf{ctr}$ maintained by $\mathcal{T}$. However, if $\mathcal{T}$ is stateless, $\mathcal{C}$ can always replay $\mathcal{S}$'s messages. In §4.4 we show how to ensure that replays do not help $\mathcal{C}$.

Since $\mathcal{S}$ and $\mathcal{T}$ derive the same randomness for each session, the (same) garbled circuit $\widetilde{f}$ can be generated by $\mathcal{T}$. Unfortunately, the weak $\mathcal{T}$ cannot store the entire $f$. Instead, $\mathcal{C}$ provides the circuit corresponding to function $f$ gate-by-gate to $\mathcal{T}$, and obtains the corresponding garbled gate of $\widetilde{f}$. The garbled gate can immediately be evaluated by $\mathcal{C}$ and needs not to be stored. $\mathcal{C}$ is prevented from providing a wrong $f$ to $\mathcal{T}$, as follows. First, $\mathcal{S}$ issues a MAC of $f$, e.g., $\mathsf{mac} = \mathsf{MAC}_k(\mathsf{sid}, f)$, where $f$ is the agreed circuit representation of the evaluated function (cf. §4.2). Further, $\mathcal{T}$ computes its version of the above MAC, $\mathsf{mac}'$, as it answers $\mathcal{C}$'s queries in computing $\widetilde{f}$. Finally, $\mathcal{T}$ reveals the decryption information $d$ that allows $\mathcal{C}$ to decrypt the output wires only if $\mathcal{C}$ provides the matching $\mathsf{mac}$.

*Garbled Inputs.* The garbled input $\widetilde{y}$ of $\mathcal{S}$ can be computed by $\mathcal{S}$ and sent to $\mathcal{C}$, requiring $|y| \cdot t$ bits communication, where $t$ is the security parameter. Alternatively, if $\mathcal{T}$ is stateful, $\mathcal{S}$ can establish a secure channel with $\mathcal{T}$, e.g., based on session key $K$, send $y$ over the channel, and have $\mathcal{T}$ output $\widetilde{y}$ to $\mathcal{C}$. This achieves the optimal communication between $\mathcal{S}$ and $\mathcal{C}$ of $|y|$ bits.

The garbling $\widetilde{x}$ of $\mathcal{C}$'s input can be transferred from $\mathcal{S}$ to $\mathcal{C}$ with a parallel OT protocol which requires $\mathcal{O}(|x|t)$ bits of communication. Alternatively, the efficient OT extension of [IKNP03] which reduces many OTs to a small number of OTs (depending on security parameter $t$) can be adopted to our token-based scenario as described in appendix §C. This reduces the communication between $\mathcal{S}$ and $\mathcal{C}$ to $\mathcal{O}(t^2)$ which is independent of the size of the input $x$.

**Extension to Covert and Malicious Parties.** Standard GC protocols for covert [GMS08] or malicious [LP07] adversaries rely on the following cut-and-choose technique. $\mathcal{S}$ creates multiple GCs $\widetilde{C}_i$, deterministically derived from random seeds $s_i$, and commits to each, e.g., by sending $\widetilde{C}_i$ or $\mathsf{H}(\widetilde{C}_i)$ to $\mathcal{C}$. In covert case, $\mathcal{C}$ asks $\mathcal{S}$ to open all but one garbled circuit $I$ by revealing the corresponding $s_{i \neq I}$. For all opened circuits, $\mathcal{C}$ computes $\widetilde{C}_i$ and checks that they match the commitments. The malicious case is similar, but $\mathcal{C}$ asks $\mathcal{S}$ to open half of the circuits, evaluates the remaining ones and chooses the majority of their results.

These protocols similarly benefit from our token-based separation of the server into $\mathcal{S}$ and $\mathcal{T}$. As in the semi-honest protocol, the GC generation can be naturally offloaded to $\mathcal{T}$, achieving corresponding computation and communication relief on the server and network resources. GC correctness verification is achieved by requesting $\mathcal{S}$ to reveal the generator seeds $s_{i \neq I}$. (Of course, these "opened" circuits are not evaluated.) Note that requirements on $\mathcal{T}$ are the same as in the semi-honest setting. Further, in both covert and malicious cases, the communication between $\mathcal{C}$ and $\mathcal{S}$ is independent of the size of $f$. The resulting communication complexity of these protocols is summarized in Table 1.

**Security Claim.** For the lack of space, in this work we present our protocols implicitly, by describing the modifications to the base protocols of [KS08]. We informally argue the security of the modifications as they are described. Formal proofs can be naturally built from proofs of [KS08] and our security arguments. At the very high level, security against $\mathcal{S}/\mathcal{T}$ follows from the underlying GC protocols, since $\mathcal{S}$ is not stronger here than in the two-party SFE setting. The additional power of $\mathcal{C}$ to control the channel between $\mathcal{S}$ and stateful $\mathcal{T}$ is negated by establishing a secure channel (§4.3). $\mathcal{C}$'s power to reset stateless $\mathcal{T}$ is addressed by ensuring that by replaying old messages $\mathcal{C}$ gets either what he already knows, or completely unrelated data (§4.4).

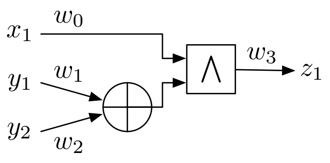
**Theorem 1.** *Assuming $\mathcal{T}$ is tamper-proof, protocols described throughout this section are secure in the semi-honest, covert, and malicious models respectively.*

## 4.2 Circuit Representation

We now describe our circuit representation format. Our criteria are compactness, the ability to accommodate free XOR gates of [KS08], and ability of $\mathcal{T}$ to process the encoding "online", i.e., with small constant memory. Recall, our $\mathcal{T}$ operates in request-response fashion. $\mathcal{C}$ incrementally, gate-by-gate, "feeds" the circuit description to $\mathcal{T}$ which responds with the corresponding garbled tables.

We consider circuits with two-input boolean gates. We note that our techniques can be naturally generalized to general circuits. A circuit can efficiently be transformed into our format as described in appendix §B.

Our format is derived from standard representations, such as that of Fairplay [MNPS04], with the necessary changes to support our requirements. For readability, we describe the format using a simple example circuit shown in Fig. 3. This circuit computes $z_1 = x_1 \wedge (y_1 \oplus y_2)$, where $x_1$ is the input bit of $\mathcal{C}$ and $y_1, y_2$ are two input bits of $\mathcal{S}$. The corresponding circuit representation shown on the right is composed from the description of the inputs, gates, and outputs as follows.



Circuit Representation:

```
1 2
3 [0] [1 2] [0001]
3
```

**Fig. 3.** Example for Circuit Representation

*Inputs and wires:* The wires $w_i$ of the circuit are labeled with their index $i = \{0, 1, ...\}$ (wires with a larger fan-out are viewed as a single wire). The first $X$ wires are associated with the input of $\mathcal{C}$, the following $Y$ wires are associated with the input of $\mathcal{S}$, and the internal wires are labeled in topological order starting from index $X + Y$ (output wires of XOR gates are not labeled, as XOR gates are incorporated into their successor gates as described in the next paragraph). The first line of the circuit description specifies $X$ and $Y$ (Fig. 3: $X = 1, Y = 2$).

*Gates* are labeled with the index of their outgoing wire; each gate description specifies its input wires. XOR gates do not have gate tables and are omitted from the description. Rather, non-XOR gates, instead of pointing to two input wires, include two input wire *lists*. If the input list contains more than one wire, these wire values are to be XORed to obtain the corresponding gate input. Gate's description concludes with its truth table. In Fig. 3, the second line describes the AND gate, which has index 3, and inputs $w_0$ and $w_1 \oplus w_2$.

*Outputs:* The circuit description concludes with $Z$ lines which contain the indices of the $Z$ output wires (Fig. 3: the only $(Z = 1)$ output wire is $w_3$).

*Large XOR sub-circuits.* In this representation, XOR gates with fan-out $> 1$ occur multiple times in the description of their successor gates. In the worst case, this results in a quadratic increase of the circuit description. To avoid this cost, we insert an identity gate after each XOR gate with a large fan-out.

## 4.3 GC Creation with Stateful Token Using Secure Counter

The main idea of our small-RAM-footprint GC generation is having $\mathcal{T}$ generate garbled tables "on the fly". This is possible, since each garbled table can be generated only given the garblings of input and output wires. In our implementation, we pseudorandomly derive the wire garbling from the session key and wire index. The rest of this section contains relevant details.

*Session Initialization.* SFE proceeds in sessions, where one session is used to securely evaluate a function once. $\mathcal{T}$ has a secure monotonic session counter $\mathsf{ctr}$ which is (irreversibly) incremented at the beginning of each session. The session id $\mathsf{sid}$ is set to the incremented state of $\mathsf{ctr}$. (We omit the discussion of synchronization of $\mathsf{ctr}$ between $\mathcal{T}$ and $\mathcal{S}$ which may happen due to communication and other errors.) Then, the session key is computed by $\mathcal{S}$ and $\mathcal{T}$ as $K = \mathsf{PRF}_k(\mathsf{sid})$ and subsequently used to provide fresh randomness to create the GC.

As required by the construction of [KS08] (cf. §2.1), the two garbled values of the same wire differ by a global difference offset $\Delta$. This offset is derived from $K$ at session initialization and kept in RAM throughout the session.

Subsequently, garbled wire values $w_i$ are derived on-the-fly from $K$ as

$$\widetilde{w}_i^0 = \mathsf{PRF}_K(i), \qquad \widetilde{w}_i^1 = \widetilde{w}_i^0 \oplus \Delta. \tag{1}$$

*Garbled Gates.* $\mathcal{T}$ receives the description of the circuit, line by line, in the format described in §4.2, and generates and outputs to $\mathcal{C}$ corresponding garbled gates, using only small constant memory. $\mathcal{T}$ first verifies that the gate with the same label had not been processed before. (Otherwise, by submitting multiple gate tables for the same gate, $\mathcal{C}$ may learn the real wire values). This is achieved by keeping the monotonically increasing processed gate counter $\mathsf{gctr}$, verifying that gate's label $\mathsf{glabel} > \mathsf{gctr}$, and setting $\mathsf{gctr} = \mathsf{glabel}$. $\mathcal{T}$ then derives and stores garblings of the gate's input and output wires according to (1). (For input lists, the wire's garbling $\widetilde{w}^0$ is computed as the XOR of garblings of the listed wires, and $\widetilde{w}^1$ is set to $\widetilde{w}^0 \oplus \Delta$. Note that this requires constant RAM.) Finally, based on these garblings, gate's garbled table is computed and output to $\mathcal{C}$.

*Garbled Outputs.* Recall, $\mathcal{T}$ must verify circuit correctness by checking $\mathsf{mac}$ generated by $\mathcal{S}$. Thus, $\mathcal{T}$ does not release the output decryption tables to $\mathcal{C}$ until after the successful check. At the same time, the check is not complete until the entire circuit had been fed to $\mathcal{T}$. To avoid having $\mathcal{T}$ store the output decryption tables or involving $\mathcal{S}$ at this stage, $\mathcal{T}$ simply encrypts the output tables using a fresh key $K'$, and outputs the key only upon a successful MAC verification.

## 4.4 GC Creation with Stateless Token (no Counter)

As discussed above, while non-volatile secure storage (the counter $\mathsf{ctr}$) is essential in our protocol of §4.3, in some cases, it may be desired to avoid its cost. We now discuss the protocol amendments required to maintain security of SFE with the support of a token whose state can be reset by, e.g., a power interruption.

First, we observe that $\mathcal{S}$ is still able to maintain state, and choose unique counters. However, $\mathcal{T}$ can no longer be assured that $\mathsf{sid}$ claimed by $\mathcal{C}$ is indeed fresh. Further, $\mathcal{T}$ does not have a source of independent randomness, and thus cannot establish a secure channel with $\mathcal{S}$, e.g., by running a key exchange.

We begin with briefly describing a replay vulnerability of our protocol of §4.3, when $\mathcal{T}$ is executed with same $\mathsf{sid}$. First, $\mathcal{C}$ properly executes SFE. Second time he runs $\mathcal{T}$ with the same $\mathsf{sid}$, but feeds $\mathcal{T}$ an incorrect circuit, receiving valid garbled tables for each of the gates, generated for the *same* wire garblings. Now, even though $\mathcal{T}$ will not accept $\mathsf{mac}$ and will not decrypt the output wires, $\mathcal{C}$ had already received them in the first execution. It is easy to see that $\mathcal{C}$ "wins".

Our solution is to ensure that $\mathcal{C}$ does not benefit from replaying $\mathcal{T}$ with the same $\mathsf{sid}$. To achieve this, we require that each wire garblings are derived from the (hash of the) entire gate description (i.e., id, truth table, and list of inputs), as described below. If $\mathcal{C}$ replays and gives a different gate description, she will not be able to relate the produced garbled table with a previous output of $\mathcal{T}$.

We associate with each wire $w_i$ a (revealed to $\mathcal{C}$) hash value $h_i$. For input wires, $h_i$ is the empty string. For each other wire $i$, $h_i$ is derived (e.g., via Random Oracle) from the description of the gate $i$ (which includes index, truth table, and list of inputs; cf. §4.2) that emits that wire: $h_i = \mathsf{H}(\langle gate\_description\rangle)$. The garbled value of wire $w_i$ now depends on its hash value $h_i$: $\widetilde{w}_i^0 = \mathsf{PRF}_K(h_i)$ and $\widetilde{w}_i^1 = \widetilde{w}_i^0 \oplus \Delta$. Finally, to enable the computation of the garbled tables, $\mathcal{C}$ must feed back to $\mathcal{T}$ the hashes $h_i$ of the input wires, and receive from $\mathcal{T}$ and keep for future use the hash of the output wire. As noted above, $\mathcal{C}$'s attempts to feed incorrect values result in the output of garbled tables that are unrelated to previous outputs of $\mathcal{T}$, and thus do not help $\mathcal{C}$.

## 5 Proof-of-concept Implementation

We have designed a proof-of-concept implementation to show the practicability of our token-assisted GC protocols of §4. In the following we describe our architecture for the stateful token case of §4.3. Extension to the stateless case is straightforward. We instantiate $\mathsf{PRF}$ with AES-128, $H$ and $\mathsf{H}$ with SHA-256, and $\mathsf{MAC}$ with AES-CMAC.

### 5.1 Architecture

Fig. 4 depicts the high level architecture of our design consisting of a two-stage pipeline and a MAC core. Stage 1 of the pipeline creates the garbled input and output values of a gate using an AES core and stage 2 computes the garbled table with a SHA core. The two-stage pipeline increases performance as two gates can be processed concurrently. The MAC core computes the authentication message $\mathsf{mac}'$ of the circuit provided by $\mathcal{C}$ (cf. §4.1).

*Design Principle.* To achieve maximum speed with minimum hardware resources, we followed a general guideline exploiting parallelism as long as it can be done without using several instances of the same algorithm. For example, we opted to compute the four entries of a garbled table with a single SHA core instead of using four parallel SHA cores which would have increased performance, but only with a significant increase in area. As the only exception, we included a separate MAC core rather than reusing the AES core of stage 1, because it would have severely complicated the control of the pipeline.

*Description of Operation.* In the session initialization (cf. §4.4), the SHA core in stage 2 derives session key $K$ and output encryption key $K'$ from key $k$ and current counter value $\mathsf{ctr} = \mathsf{sid}$ which is used as key for the AES core. Then, the key difference $\Delta$ is derived with the AES core and stored in a register. The circuit is provided gate-by-gate into the input buffer in the format described in §4.2 (gate table denoted by $T_i$ in Fig. 4). Stage 1 starts to process a gate by deriving the garbled output value $\widetilde{w}_i^0$. Then, the two garbled inputs of the gate ($\widetilde{L}_i^0, \widetilde{R}_i^1$ in Fig. 4) are derived by XORing the garblings listed in the input wire lists one-by-one (see §4.3). When all garblings are derived they are forwarded to stage 2 and stage 1 processes the next gate. Stage 2 computes the garbled table

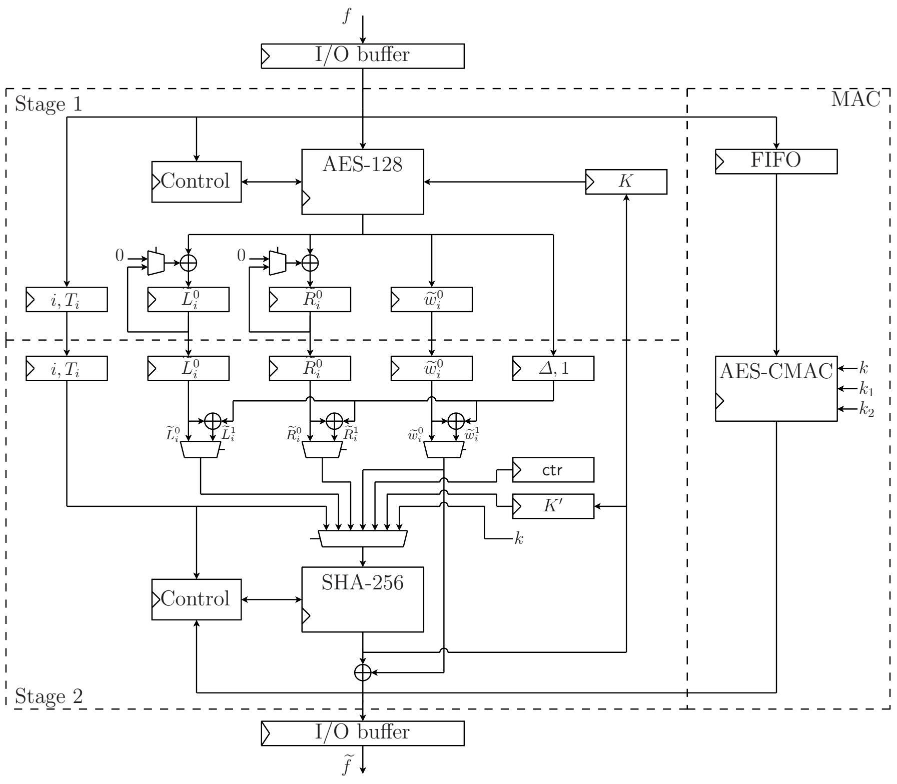


**Fig. 4.** Simplified architectural diagram of our proof-of-concept implementation. Selectors of multiplexers and write enables of registers are set by additional control logics.

and the encrypted output decryption tables and writes them into the output buffer. The MAC core operates independently from the two-stage pipeline.

## 5.2 Prototype Implementation

We implemented our architecture in VHDL.

*Implementation Details.* For the AES core we chose an iterative design of AES-128 with a latency of 10 clock cycles per encryption. The core includes an online key scheduling unit. The S-boxes are implemented as suggested in [Can05]; otherwise, the core is a straightforward implementation of the standard [NIS01]. The SHA core implements SHA-256 with a latency of 67 clock cycles per 512-bit block. The core is a straightforward iterative design of the standard [NIS02]. The MAC core includes an AES core implemented as above; otherwise the core is a straightforward implementation of AES-CMAC [SPLI06]. As the subkeys, $k_1$ and $k_2$, depend only on the key $k$ they were precomputed and hardwired in the design.

*FPGAs.* We compiled the VHDL code for a low-end FPGA, the Altera Cyclone II EP2C20F484C7 FPGA, with Quartus II, version 8.1 (2008). We emphasize that this FPGA is for prototyping only, as it lacks secure embedded non-volatile memory for storing $\mathsf{ctr}$ (e.g., the Xilinx Spartan-3AN FPGAs has integrated Flash memory for this). The resulting area and memory requirements are listed in Table 3. The design occupies 60 % of logic cells and 21 % of memory blocks available on the device and runs at 66 MHz (the critical path for clock frequency is in the AES core). These results show that the design is, indeed, feasible for a low-cost implementation, for example, with low-cost FPGAs which, in turn, is mandatory for the practicability of the token-based scheme.

**Table 3.** Results on an Altera Cyclone II FPGA (the hierarchy is as shown in Fig. 4).

| **Entity** | Stage 1 | Stage 2 | MAC | IO | Total |
|---|---|---|---|---|---|
| **Area** (Logic cells) | 3317 (30 %) | 4539 (40 %) | 3059 (27 %) | 263 (3 %) | 11231 (60 %) |
| **Memory** (M4K) | 0 (0 %) | 8 (73 %) | 1 (9 %) | 2 (18 %) | 11 (21 %) |

*Smart Cards.* In particular, we note that the requirements are sufficiently low also for contemporary smart card technologies, because AES-128 and SHA-256 require only about 3,400 and 11,000 gates, respectively [FW07]. As our protocol requires no public-key operations on the token, small smart cards are sufficient.

**Performance.** We determined the latency of our implementation with ModelSim, version 6.3g (2008). Overall, the latency is given as $\#\mathsf{clock\_cycles} = 158G_1 + 312G_2 + 154O + 150$, where $G_1, G_2$ is the number of 1-input gates respectively 2-input gates and $O$ is the number of outputs, assuming that each gate has at most 21 inputs in its input lists (if more, stage 2 needs to wait for stage 1) and that data I/O does not introduce additional delays. If we use a correlation robust hash function instead of RO, the coefficient for $G_2$ would roughly double for up to 42 inputs (cf. §2.1).

*Example 1.* Our implementation generates a GC for 16-bit comparison ($G_1 = 0, G_2 = 16, O = 1$) in 5,296 clock cycles ($\approx$80 $\mu$s with 66 MHz clock). In Software, this takes roughly 0.5 s on an Intel Core 2 6420 at 2.13 GHz [LPS08].

*Example 2.* Generating a GC for AES-128 encryption ($G_1 = 12614$, $G_2 = 11334$, $O = 128$) takes 5,549,082 clock cycles ($\approx$84 ms with 66 MHz clock). In Software, this takes approximately 1 s on an Intel Core 2 Duo at 3.0 GHz [PSSW09].

We note that the optimization for large XOR sub-circuits described in §4.2 dramatically reduces the amount of communication between $\mathcal{C}$ and $\mathcal{T}$: When using this optimization, the size of the AES circuit of Example 2 is $|C| = 1.1$ MB and the garbled AES circuit has size $|\widetilde{C}| = 1.1$ MB. Without this optimization, the circuit has no more 1-input gates ($G_1 = 0$) which results in a faster creation ($3,556,070$ clock cycles), evaluation, and size of the garbled circuit ($|\widetilde{C}| \approx$

0.7 MB). However, the size of the circuit is drastically larger ($|C| = 94.5$ MB) which might be a bottleneck if the communication between $\mathcal{C}$ and $\mathcal{T}$ is slow.

**Acknowledgements.** We would like to thank Wilko Henecka for preparing test circuits, and Ivan Damgård and reviewers of FC'10 for their helpful comments.

## References

[AIR01] W. Aiello, Y. Ishai, and O. Reingold. Priced oblivious transfer: How to sell digital goods. In *EUROCRYPT'01*, volume 2045 of *LNCS*, pages 119–135. Springer, 2001.

[Ber91] C. L. Berman. Circuit width, register allocation, and ordered binary decision diagrams. *IEEE Trans. on CAD of Integrated Circuits and Systems*, 10(8):1059–1066, 1991.

[BFK$^+$09] M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider. Secure evaluation of private linear branching programs with medical applications. In *ESORICS'09*, volume 5789 of *LNCS*, pages 424–439. Springer, 2009.

[CAC$^+$81] G. J. Chaitin, M. A. Auslander, A. K. Chandra, J. Cocke, M. E. Hopkins, and P. W. Markstein. Register allocation via coloring. *Comput. Lang.*, 6(1):47–57, 1981.

[Can05] D. Canright. A very compact S-box for AES. In *Cryptographic Hardware and Emb. Systems (CHES'05)*, volume 3659 of *LNCS*, pages 441–456. Springer, 2005.

[CGS08] N. Chandran, V. Goyal, and A. Sahai. New constructions for UC secure computation using tamper-proof hardware. In *EUROCRYPT'08*, volume 4965 of *LNCS*, pages 545–562. Springer, 2008.

[CLOS02] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable two-party and multi-party secure computation. In *STOC'02*, pages 494–503, 2002.

[DNW09] I. Damgård, J. B. Nielsen, and D. Wichs. Universally composable multiparty computation with partially isolated parties. In *Theory of Cryptography (TCC'09)*, volume 5444 of *LNCS*, pages 315–331. Springer, 2009.

[FFP$^+$06] M. Fort, F. C. Freiling, L. D. Penso, Z. Benenson, and D. Kesdogan. Trustedpals: Secure multiparty computation implemented with smart cards. In *ESORICS'06*, volume 4189 of *LNCS*, pages 34–48. Springer, 2006.

[FW07] M. Feldhofer and J. Wolkerstorfer. Strong crypto for RFID tags — a comparison of low-power hardware implementations. In *IEEE Symp. Circuits and Systems (ISCAS'07)*, pages 1839–1842, 2007.

[GMS08] V. Goyal, P. Mohassel, and A. Smith. Efficient two party and multi party computation against covert adversaries. In *EUROCRYPT'08*, volume 4965 of *LNCS*, pages 289–306. Springer, 2008.

[Goo09] Google Health, 2009. `https://www.google.com/health`.

[GT08] V. Gunupudi and S. Tate. Generalized non-interactive oblivious transfer using count-limited objects with applications to secure mobile agents. In *Financial Crypto (FC'08)*, volume 5143 of *LNCS*, pages 98–112. Springer, 2008.

[HL08] C. Hazay and Y. Lindell. Constructions of truly practical secure protocols using standard smartcards. In *Proc. ACM CCS*, pages 491–500. ACM, 2008.

[HMU05] D. Hofheinz, J. Müller-Quade, and D. Unruh. Universally composable zero-knowledge arguments and commitments from signature cards. In *Central European Conference on Cryptology (MoraviaCrypt'05)*, 2005.

[IKNP03] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank. Extending oblivious transfers efficiently. In *Adv. in Cryp. – CRYPTO'03*, volume 2729 of *LNCS*. Springer, 2003.

[IS05] A. Iliev and S. Smith. More efficient secure function evaluation using tiny trusted third parties. Technical Report TR2005-551, Dartmouth College, Computer Science, Hanover, NH, July 2005.

[JKSS10] Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. Embedded SFE: Offloading server and network using hardware tokens. In *14th International Conference on Financial Cryptography and Data Security (FC'10)*, LNCS. Springer, January 25-28, 2010.

[Kat07] J. Katz. Universally composable multi-party computation using tamper-proof hardware. In *EUROCRYPT'07*, pages 115–128. Springer, 2007.

[KBC97] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-hashing for message authentication. RFC 2104 (Informational), February 1997. `http://tools.ietf.org/html/rfc2104`.

[KS08] V. Kolesnikov and T. Schneider. Improved garbled circuit: Free XOR gates and applications. In *ICALP'08*, volume 5126 of *LNCS*, pages 486–498. Springer, 2008.

[LP07] Y. Lindell and B. Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. In *EUROCRYPT'07*, volume 4515 of *LNCS*, pages 52–78. Springer, 2007.

[LP09] Y. Lindell and B. Pinkas. A proof of Yao's protocol for secure two-party computation. *Journal of Cryptology*, 22(2):161–188, 2009. Cryptology ePrint Archive: Report 2004/175.

[LPS08] Y. Lindell, B. Pinkas, and N. Smart. Implementing two-party computation efficiently with security against malicious adversaries. In *Security and Cryptography for Networks (SCN'08)*, volume 5229 of *LNCS*, pages 2–20. Springer, 2008.

[MNPS04] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella. Fairplay — a secure two-party computation system. In *USENIX*, 2004.

[MS08] T. Moran and G. Segev. David and goliath commitments: UC computation for asymmetric parties using tamper-proof hardware. In *EUROCRYPT'08*, volume 4965 of *LNCS*, pages 527–544. Springer, 2008.

[NIS01] NIST, U.S. National Institute of Standards and Technology. Federal information processing standards (FIPS 197). Advanced Encryption Standard (AES), November 2001. `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

[NIS02] NIST, U.S. National Institute of Standards and Technology. Federal information processing standards (FIPS 180-2). Announcing the Secure Hash Standard, August 2002. `http://csrc.nist.gov/publications/fips/fips180-2/fips-180-2.pdf`.

[NP01] M. Naor and B. Pinkas. Efficient oblivious transfer protocols. In *ACM-SIAM Symposium On Discrete Algorithms (SODA'01)*, pages 448–457. SIAM, 2001.

[PSSW09] B. Pinkas, T. Schneider, N. P. Smart, and S. C. Williams. Secure two-party computation is practical. In *ASIACRYPT'09*, LNCS. Springer, 2009.

[Sha49] C. E. Shannon. The synthesis of two-terminal switching circuits. *Bell Systems Technical Journal*, 28(1):59–98, 1949.

[SPLI06] JH. Song, R. Poovendran, J. Lee, and T. Iwata. The AES-CMAC Algorithm. RFC 4493 (Informational), June 2006. `http://tools.ietf.org/html/rfc4493`.

[SS02] Y. N. Srikant and P. Shankar, editors. *The Compiler Design Handbook: Optimizations and Machine Code Generation.* CRC Press, 2002.

[Tur96] B. C. H. Turton. Extending quine-mccluskey for exclusive-or logic synthesis. *IEEE Transactions on Education*, 39:81–85, 1996.

[TV09] S. Tate and R. Vishwanathan. Improving cut-and-choose in verifiable encryption and fair exchange protocols using trusted computing technology. In *Data and Applicat. Sec. (DBSec'09)*, volume 5645 of *LNCS*, pages 252–267. Springer, 2009.

[Yao86] A. C. Yao. How to generate and exchange secrets. In *IEEE Symposium on Foundations of Computer Science (FOCS'86)*, pages 162–167. IEEE, 1986.

## A Further Optimizations

In order to allow $\mathcal{C}$ to evaluate the garbled circuit on-the-fly without caching the garbled gates, the gates of the circuit must be given in topologic order, i.e., all gates on which a gate depends have to occur before. As for most circuits many topologic orders exist, one can choose a specific topologic order according to further optimizations. We give two examples in the following – optimize $\mathcal{C}$'s memory requirements for GC evaluation (appendix §A.1) or reduce $\mathcal{T}$'s runtime by caching intermediate values (appendix §A.2).

### A.1 Optimizing Memory of Client

For evaluating the garbled circuit, $\mathcal{C}$ starts with the garbled values of the inputs. Then, $\mathcal{C}$ obtains the garbled gates one-by-one from the token and evaluates them. The obtained garbled output for the gate needs to be stored in $\mathcal{C}$'s memory until it is used the last time as input into a garbled gate.

This allows to find a good topologic order of the circuit which requires less memory for storing the intermediate results.

As pointed out in [Ber91], the problem of finding a topologic order of a circuit that minimizes the needed amount of memory to store intermediate values is equivalent to the register allocation problem which is well-studied in the context of compilers. In fact, algorithms for register allocation [CAC$^+$81,SS02] can be used to find an optimal respectively good topologic order of the circuit which reduces the amount of memory needed for its evaluation.

In the worst case, the memory needed to evaluate a circuit $C$ is linear in the circuit size as one might need to keep garbled values of many wires. Fig. 5 shows an (artificially constructed) example circuit with $k$ gates which requires $\Theta(k)$ memory for evaluation.

### A.2 Optimizing Runtime of Token by Caching

During creation of the garbled circuit, the token $\mathcal{T}$ derives the garbled values corresponding to the gates' inputs and outputs with a PRF. If the garbled value

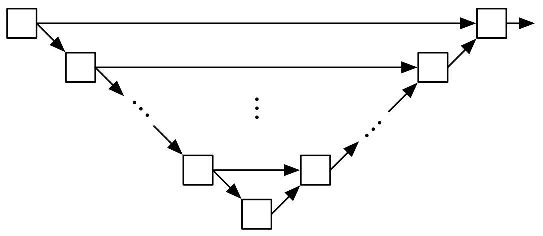


**Fig. 5.** Circuit with $k$ gates which requires $\Theta(k)$ memory for evaluation.

has already been derived before and stored in a cache, the garbled value does not need to be derived again. When the garbled values are stored into or loaded from the cache can be encoded in the description of the circuit provided by $\mathcal{C}$.

*Performance Improvements by Caching.* At a first glance it seems that the cache provides the possibility for a time-memory-tradeoff. This is clearly the case if $\mathcal{T}$ allows sequential execution of instructions only (e.g., in a single-threaded software implementation on a smart card) as each cache hit results in reduced computation time. However, if $\mathcal{T}$ allows parallel execution (e.g., on FPGAs, ASICs or CPUs with multiple cores), the garbled values can be derived in parallel to creating the garbled tables. As demonstrated in our FPGA prototype implementation in §5, the derivation of the garbled values using AES (10 cycles in our implementation) is substantially faster than creating the garbled tables using SHA (70 cycles in our implementation). In this setting, only gates with many inputs would benefit from caching.

**Cache Sizes.** If each garbled value should be derived only once and taken from the cache every time it is used afterwards, the cache needs to have size $\mathcal{O}(|f|)$. In practice, the size of the cache is however bounded to a constant number of cache entries.

*Cache with constant size.* To determine a good ordering of the gates which maximizes the number of cache hits one can use standard algorithms for instruction scheduling and register allocation (instructions correspond to gates and registers to cache entries) [SS02].

*Cache with size* 1. In many cases, a cache with only one cache entry is sufficient already. This is due to the fact that many commonly used functionalities (e.g., addition or comparison) are composed from a line of gates in which the output of a gate directly serves as the input into the next gate.

The following efficient algorithm (time and space complexity in $\mathcal{O}(|f|)$) determines a topological order with many hits for the one entry cache: Insert – starting from the output gates – an edge to each of the gates whose outputs are input into the current gate. Afterwards run a depth-first search on the outputs which marks a gate as visited and visits all successor gates which have not been visited yet. After having visited all successor gates, the gate is output as next in the topologic order. This algorithm eliminates “dead” gates and results in many cache hits for the one entry cache.

## B Transformation of Circuit into Token Format

In order to convert a given circuit with $n$-input gates into the token format described in §4.2 the gates are first decomposed into 2-input gates and afterwards the XOR gates are grouped together:

*Decomposition into* 2*-input gates.* Decomposing the $n$-input gates of a circuit into multiple 2-input gates can be done in a straight-forward way using Shannon’s expansion theorem [Sha49] or the QuineMcCluskey algorithm which results in smaller circuits [Tur96]. For small $n$ (e.g., for the very common case of $n = 3$), the optimal replacement can be found via brute-force enumeration of all possibilities [PSSW09].

*Grouping of XOR gates.* The XOR gates can be grouped together as follows: To each input wire and each output wire of a non-XOR gate $i$ we assign the set $\{i\}$. Afterwards we transfer the gates of the circuit in topological order and annotate to the output wire of each XOR gate the following set which is computed from the sets of its input wires $S_1$, $S_2$ as $S = S_1 \oplus S_2 := (S_1 \cup S_2) \setminus (S_1 \cap S_2)$. Finally, the remaining non-XOR gates are output in the token format using the sets associated to the input wires which contain those wires which need to be XORed together for the specific input. As merging two sets of size at most $|C|$ entries each can be done in $\mathcal{O}(|C|)$ operations, the overall complexity of this algorithm is in $\mathcal{O}(|C|^2)$.

## C Extending OT Efficiently with Token

As described in §4.1, $\mathcal{C}$ needs to obtain the garbled values $\widetilde{x}$ corresponding to her input with a parallel OT protocol.

The efficient OT extension of [IKNP03] for *semi-honest receiver* $\mathcal{C}$ can be used to replace the possibly huge number of $|x|$ parallel OTs with a substantially smaller number of $t$ OTs only, where $t$ is a security parameter. As the token $\mathcal{T}$ is computationally weak and can not perform public-key operations, the $t$ real OTs in the protocol of [IKNP03] are performed between the computationally strong devices $\mathcal{C}$ and $\mathcal{S}$. Afterwards, $\mathcal{S}$ sends its state, i.e., the values obtained in the parallel OT protocol to $\mathcal{T}$ over a secure channel. This requires $\mathcal{O}(t^2)$ communication from $\mathcal{S}$ to $\mathcal{T}$ (forwarded by $\mathcal{C}$). Finally, $\mathcal{T}$ completes the protocol with $\mathcal{C}$ which requires several invocations of a correlation robust hash function (e.g., SHA-256) only, but no more public-key operations.

The fully secure OT extension protocol of [IKNP03] which is secure against *malicious receiver* $\mathcal{C}$ requires additional cut-and-choose which results in correspondingly increased communication between $\mathcal{C}$ and $\mathcal{S}$. Nevertheless, the communication between $\mathcal{C}$ and $\mathcal{S}$ remains independent of the number of inputs $|x|$.